What is claimed is:

1. An authentication system for mutual authentication between a terminal and a server characterized by the fact that the terminal comprises:

a memory means that pre-stores an authentication information P' for terminal storage;

a concatenation means that yields a value P using a specific calculation formula in response to the input of the authentication information P' read from the memory means and a password entered for authentication;

a mask operation means that yields a value Y1 using a specific calculation formula with the input value P and an internally generated random number, and then sends Y1 to the server; and

a master key generation means that yields a value MK using a specific calculation formula with the input value P, an internally generated random number and a value Y2 received from a server that comprises:

a memory means that pre-stores a password verification data H for server registeration;

a mask operation means that yields a value Y2 using a specific calculation formula with the input of the password verification data H read from the memory means and an internally generated random number, and then sends Y2 to the terminal; and

a master key generation means that yields a value MK using a specific calculation formula with the input of the password verification data H, an internally generated random number and the value Y1 received from the terminal.

2. The authentication system according to Claim 1 characterized by further comprising a data extension means that yields the password verification data H and the authentication information P' based on a password previously-determined by the user.

3. The authentication system according to Claim 1 or 2 characterized by the fact that the terminal further comprises:

an authentication result verification means that yields a value V1 using a specific calculation formula with the input of the value MK, sends V1 to the server and compares a

value V2 received from the server with a value V2 obtained using a specific calculation formula with the input of the value MK and, if they match, authenticates the server,

and the server further comprises:

an authentication result verification means that yields a value V2 using a specific calculation formula with the input of the value MK, sends V2 to the terminal and compares a value V1 received from the terminal with a value V1 obtained using a specific calculation formula with the input of the value MK and, if they match, authenticates the terminal.

4. The authentication system according to Claim 3 characterized by the fact that each of the terminal and the server comprises a session key generation means that generates a session key when they are mutually authenticated.

5. The authentication system according to any of Claims 1 to 4 characterized by the fact that the authentication information P' is a polynomial equation.

6. The authentication system according to any of Claims 1 to 4 characterized by the fact that the authentication information P' is a polynomial equation and a hash function.

7. The authentication system according to any of Claims 1 to 4 characterized by the fact that the authentication information P' is a hash function.

8. The authentication system according to any of Claims 1 to 4 characterized by the fact that the authentication information P' is a pseudo random number generator.

9. An authentication program that runs on the terminal of an authentication system for mutual authentication between a terminal and a server characterized by the fact that the program allows a computer to execute:

a memory process to pre-store an authentication information P' for terminal storage;

a concatenation process to yield a value P using a specific calculation formula with the input of the stored authentication information P' and a password entered for authentication;

a mask operation process to yield a value Y1 using a specific calculation formula with

the input value P and an internally generated random number, and then send Y1 to the server; and

a master key generation process to yield a value MK using a specific calculation formula with the input value P, an internally generated random number and a value Y2 received from the server.

10. The authentication program according to Claim 9 characterized by the fact that the program further allows a computer to execute a data extension process to yield the authentication information P' based on a password previously-determined by the user.

11. The authentication program according to Claim 9 or 10 characterized by the fact that the program further allows a computer to execute an authentication result verification process to yield a value V1 using a specific calculation formula with the input of the value MK, send V1 to the server and compare a value V2 received from the server with a value V2 obtained using a specific calculation formula with the input of the value MK and, if they match, authenticate the server.

12. An authentication program that runs on the server of an authentication system for mutual authentication between a terminal and a server characterized by the fact that the program allows a computer to execute:

a memory process to pre-store a password verification data H for server registeration;

a mask operation process to yield a value Y2 using a specific calculation formula with the input of the stored password verification data H and an internally generated random number, and then send Y2 to the terminal; and

a master key generation process to yield a value MK using a specific calculation formula with the input of the password verification data H, an internally generated random number and a value Y1 received from the terminal.

13. The authentication program according to Claim 12 characterized by the fact that the program further allows a computer to execute a data extension process to yield the password verification data H based on a password previously-determined by the user.

14. The authentication program according to Claim 12 or 13 characterized by the fact that the program further allows a computer to execute an authentication result verification process to yield a value V2 using a specific calculation formula with the input of the value MK, send V2 to the terminal and compare a value V1 received from the terminal with a value V1 obtained using a specific calculation formula with the input of the value MK and, if they match, to authenticate the terminal.

15. The authentication program according to Claim 11 or 14 characterized by the fact that each of the terminal and the server comprises a session key generation process to generate a session key when they are mutually authenticated.

16. The authentication program according to any of Claims 9 to 15 characterized by the fact that the authentication information P' is a polynomial equation.

17. The authentication program according to any of Claims 9 to 15 characterized by the fact that the authentication information P' is a polynomial equation and a hash function.

18. The authentication program according to any of Claims 9 to 15 characterized by the fact that the authentication information P' is a hash function.

19. The authentication program according to any of Claims 9 to 15 characterized by the fact that the authentication information P' is a pseudo random number generator.

20. The authentication system according to Claim 2 characterized by the fact that the terminal comprises:

a generation means that generates an update information T' ; and

an update information generation means that yields a password verification data H' for server update and a new authentication information P' using a specific calculation formula with the input of authentication information P' stored in the memory means and the update information T', sends the password verification data H' for server update to the server, and stores the new authentication information P' in the memory means,

and the server comprises:

an update information generation means that yields a new password verification data H using a specific calculation formula with the input of password verification data H' for server update sent from the terminal and password verification data H stored in the memory means, and then updates the password verification data H stored in the memory means.

21. The authentication system according to Claim 2 characterized by the fact that the terminal comprises:

a generation means that generates a secret information S'; and

an update information generation means that yields a password verification data H' for server update and a new authentication information P' using a specific calculation formula with the input of an authentication information P' stored in the memory means, the secret information S' and a new password, sends the password verification data H' for server update to the server, and then stores the new authentication information P' in the memory means,

and the server comprises:

an update information generation means that yields a new password verification data H using a specific calculation formula with the input of password verification data H' for server update sent from the terminal and password verification data H stored in the memory means, and then updates the password verification data H stored in the memory means.

22. An authentication system for mutual authentication between a terminal and a server characterized by the fact that the terminal comprises:

a memory means that pre-stores an authentication information P' for terminal storage and an RSA public key (N, e);

a concatenation means that yields a value W using a specific calculation formula with the input of the authentication information P' read from the memory means and a password entered for authentication; and

a mask operation means that yields a value Z using a specific calculation formula with the input of the value W, RSA public key (N, e) read from the memory means and an internally generated random number T, and then sends Z to the server,

and the server comprises:

a memory means that pre-stores a password verification data H for server registration and an RSA private key (N, d); and

a master key generation means that yields a value T using a specific calculation formula with the input of the password verification data H and RSA private key (N, d) read from the memory means and a value Z received from the terminal.

23. The authentication system according to Claim 22 characterized by further comprising a data extension means that yields the password verification data H and the authentication information P' based on a password previously-determined by the user.

24. The authentication system according to Claim 22 characterized by further comprising an RSA key generation means that yields the RSA public key (N, e) and the RSA private key (N, d).

25. The authentication system according to Claim 22, 23 or 24 characterized by the fact that the terminal further comprises:

an authentication result verification means that compares a value V2 received from the server with a value V2 obtained using a specific calculation formula with the input of the random number T and, if they match, authenticates the server; and

a verifier generation means that yields a value V1 using a specific calculation formula with the input of the random number T and sends V1 to the server,

and the server further comprises:

a verifier generation means that yields a value V2 using a specific calculation formula with the input of the value T and sends V2 to the terminal; and

an authentication result verification means that compares a value V1 received from the terminal with a value V1 obtained using a specific calculation formula with the input of the value T and, if they match, authenticates the terminal.

26. The authentication system according to Claim 25 characterized by the fact that each of the terminal and the server comprises a session key generation means that generates a session key when they are mutually authenticated.

27. The authentication system according to any of Claims 22 to 26 characterized by the fact that the authentication information P' is a polynomial equation and an FDH function.

28. The authentication system according to any of Claims 22 to 26 characterized by the fact that the authentication information P' is an FDH function.

29. The authentication system according to any of Claims 22 to 26 characterized by the fact that the RSA public key (N, e) uses secure communication.

30. The authentication system according to any of Claims 22 to 26 characterized by the fact that the RSA public key (N, e) uses insecure communication.

31. An authentication program that runs on a terminal of an authentication system for mutual authentication between a terminal and a server characterized by the fact that the program allows a computer to execute:

a memory process to pre-store an authentication information P' for terminal storage and an RSA public key (N, e);

a concatenation process to yield a value W using a specific calculation formula with the input of the stored authentication information P' and a password entered for authentication; and

a mask operation process to yield a value Z using a specific calculation formula with the input of the value W, the stored RSA public key (N, e), and an internally generated random number T, and then send Z to the server.

32. The authentication program according to Claim 31 characterized by the fact that the program further allows a computer to execute a data extension process to yield authentication information P' based on a password previously-determined by the user.

33. The authentication program according to Claim 31 characterized by the fact that the program further allows a computer to execute an RSA key generation process to yield the RSA public key (N, e).

34. The authentication program according to Claim 31, 32 or 33 characterized by the fact that the program further allows a computer to execute:

an authentication result verification process to compare a value V2 received from the server with a value V2 obtained using a specific calculation formula with the input of the random number T and, if they match, authenticate the server; and

a verifier generation process to yield a value V1 using a specific calculation formula with the input of the random number T and send V1 to the server.

35. An authentication program that runs on a server of an authentication system for mutual authentication between a terminal and a server characterized by the fact that the program allows a computer to execute:

a memory process to pre-store a password verification data H for server registration and an RSA private key (N, d); and

a master key generation process to yield a value T using a specific calculation formula with the input of the stored password verification data H, RSA private key (N, d) and a value Z received from the terminal.

36. The authentication program according to Claim 35 characterized by the fact that the program further allows a computer to execute a data extension process to yield the password verification data H based on a password previously-determined by the user.

37. The authentication program according to Claim 35 characterized by the fact that the program further allows a computer to execute an RSA key generation process to yield the RSA private key (N, d).

38. The authentication program according to Claim 35, 36, or 37 characterized by the fact that the program further allows a computer to execute:

a verifier generation process to yield a value V2 using a specific calculation formula with the input of the value T and send V2 to the terminal; and

an authentication result verification process to compare a value V1 received from the server with a value V1 obtained using a specific calculation formula with the input of the

value T and, if they match, to authenticate the terminal.

39. The authentication program according to Claim 34 or 38 characterized by the fact that each of the terminal and the server comprises a session key generation process to generate a session key when they are mutually authenticated.

40. The authentication program according to any of Claims 31 to 39 characterized by the fact that the authentication information P' is a polynomial equation and an FDH function.

41. The authentication program according to any of Claims 31 to 39 characterized by the fact that the authentication information P' is an FDH function.

42. The authentication program according to any of Claims 31 to 39 characterized by the fact that the RSA public key (N, e) uses secure communication.

43. The authentication program according to any of Claims 31 to 39 characterized by the fact that the RSA public key (N, e) uses insecure communication.

44. The authentication system according to Claim 23 characterized by the fact that the terminal comprises:

a generation means that generates an update information T' ; and

an update information generation means that yields a password verification data H' for server update and a new authentication information P' using a specific calculation formula with the input of an authentication information P' stored in the memory means and the update information T', sends the password verification data H' for server update to the server, and stores the new authentication information P' in the memory means,

and the server comprises:

an update information generation means that yields a new password verification data H using a specific calculation formula with the input of the password verification data H' for server update sent from the terminal and a password verification data H stored in the memory means, and then updates the password verification data H stored in the memory means.

45. The authentication system according to Claim 22 characterized by the fact that the terminal comprises:

an update information generation means that yields a new authentication information P' using a specific calculation formula with the input of an authentication information P' stored in the memory means and the random number T, and then stores the new authentication information P' in the memory means,

and the server comprises:

an update information generation means that yields a new password verification data H using a specific calculation formula with the input of a password verification data H stored in the memory means and a value T yielded by the master key generation means, and then updates the password verification data H stored in the memory means.

46. The authentication system according to Claim 23 characterized by the fact that the terminal comprises:

a generation means that generates a secret information S'; and

an update information generation means that yields a password verification data H' for server update and a new authentication information P' using a specific calculation formula with the input of authentication information P' stored in the memory means, the secret information S' and a new password, sends the password verification data H' for server update to the server, and then stores the new authentication information P' in the memory means,

and the server comprises:

an update information generation means that yields a new password verification data H using a specific calculation formula with the input of password verification data H' for server update sent from the terminal and password verification data H stored in the memory means, and then updates the password verification data H stored in the memory means.

47. A remotely-distributed storage system that conducts mutual authentication between a terminal and multiple servers, distributes terminal data to be stored, and stores them on the servers characterized by the fact that the terminal comprises:

a data extension means that yields a password verification data H for server registeratioin and an authentication information P' for terminal storage based on a password previously-determined by the user;

a memory means that pre-stores the authentication information P' yielded by the data extension means;

a concatenation means that yields a value P using a specific calculation formula with the input of the authentication information P' read from the memory means and a password entered for authentication;

a mask operation means that yields a value Y1 using a specific calculation formula with the input value P and an internally generated random number, and then sends Y1 to the server;

a master key generation means that yields a value MK using a specific calculation formula with the input of the value P, an internally generated random number and a value Y2 received from the server;

an authentication result verification means that yields a value V1 using a specific calculation formula with the input of the value MK, sends V1 to the server and compares a value V2 received from the server with the value V1 and, if they match, authenticates the server;

a session key generation means that generates the same number of session keys SK as the number of servers when the servers are authenticated;

a data dividing means that divides the data to be stored and yields the same number of divided data as the number of authenticated servers;

a data storing means that encodes the divided data and an identification information for identifying the data to be stored using the session keys SK shared with the storing servers, and then sends them to the servers; and

a data decoding means that receives the divided data from the servers where the data are stored, and then decodes the stored data,

and the server comprises:

a memory means that pre-stores a password verification data H yielded by the data extension means;

a mask operation means that yields a value Y2 using a specific calculation formula with the input of a password verification data H read from the memory means and an

internally generated random number, and then sends Y2 to the terminal;

a master key generation means that yields a value MK using a specific calculation formula with the input of the password verification data H, an internally generated random number and a value Y1 received from the terminal;

an authentication result verification means that yields a value V2 using a specific calculation formula with the input of the value MK, sends Y2 to the terminal and compares a value V1 received from the terminal with the value V2 and, if they match, authenticates the terminal;

a session key generation means that generates a session key SK when the terminal is authenticated;

a data receiving means that receives divided data from the terminal;

a data storing means that stores the divided data; and

a data transfer means that reads the divided data stored in the data storing means and sends them to the terminal.

48. The remotely-distributed storage system according to Claim 47 characterized by the fact that some of the divided data are stored on the terminal.

49. A remotely-distributed storage program that runs on a terminal of a remotely-distributed storage system that conducts mutual authentication between a terminal and multiple servers, distributes terminal data to be stored, and stores them on the servers characterized by the fact that the program allows a computer to execute:

a data extension process to yield a password verification data H for server registeration and an authentication information P' for terminal storage based on a password previously-determined by the user;

a memory process to pre-store the authentication information P' yielded in the data extension process;

a concatenation process to yield a value P using a specific calculation formula with the input of the authentication information P' read from the memory process and a password entered for authentication;

a mask operation process to yield a value Y1 using a specific calculation formula with the input of value P and an internally generated random number, and then send Y1 to the

server;

a master key generation process to yield a value MK using a specific calculation formula with the input of the value P, an internally generated random number and a value Y2 received from the server;

an authentication result verification process to yield a value V1 using a specific calculation formula with the input of the value MK, send V1 to the server and compare a value V2 received from the server with the value V1 and, if they match, authenticate the server;

a session key generation process to generate the same number of session keys SK as the number of servers when the servers are authenticated;

a data dividing process to divide the data to be stored and yield the same number of divided data as the number of authenticated servers;

a data storing process to encode the divided data and an identification information for identifying the data to be stored using the session keys SK shared with the storing servers, and then send them to the servers; and

a data decoding process to receive the divided data from the servers where the data are stored, and then decode the stored data.

50. A remotely-distributed storage program that runs on a server of a remotely-distributed storage system that conducts mutual authentication between a terminal and multiple servers, distributes terminal data to be stored, and stores them on the servers characterized by the fact that the program allows a computer to execute:

a memory process to pre-store a password verification data H yielded in a data extension process;

a mask operation process to yield a value Y2 using a specific calculation formula with the input of a password verification data H read from the memory process and an internally generated random number, and then send Y2 to the terminal;

a master key generation process to yield a value MK using a specific calculation formula with the input of the password verification data H, an internally generated random number and a value Y1 received from the terminal;

an authentication result verification process to yield a value V2 using a specific calculation formula with the input of the value MK, send V2 to the terminal and compare a

value V1 received from the terminal with the value V2 and, if they match, to authenticate the terminal;

a session key generation process to generate a session key SK when the terminal is authenticated;

a data receiving process to receive divided data from the terminal;

a data storing means to store the divided data; and

a data transfer process to read the divided data stored in the data storing process and send them to the terminal.